AMENDMENTS TO THE SPECIFICATION:

Please replace the paragraph beginning on page 3, line 3 with the following amended paragraph:

However, although the conventional RSA encryption scheme as described above has a high performance in terms of data secrecy and has a simple algorithm ~~algorism~~, its security depends on the difficulty of factoring a product n of two prime numbers p and q. Therefore, it is necessary to use about 200-digit n in the decimal system, and there is the problem that it is very difficult to perform modulo n exponentiation, which are necessary for encryption and decryption processes.

Please replace the paragraph beginning on page 3, line 17 with the following amended paragraph:

An object of the present invention is to suggest a secret cryptosystem of an extremely simple public key, which simplifies its algorithm ~~algorism~~, while maintaining a security equivalent to the RSA encryption scheme, and to provide an encrypting device which can perform encryption by simple calculations, a decrypting device which can perform decryption by simple calculations, a cryptosystem including the same devices, an encrypting method, and a decrypting method.

Please replace the paragraph beginning on page 20, line 6 with the following amended paragraph:

The cryptosystem of the present embodiment, which has the same basic principle as that of the cryptosystem in the Embodiment 1, can make its algorithm ~~algorism~~ simpler under the condition that a size b of a private key p is limited in relation to a message m.

Please replace the paragraph beginning on page 43, line 15 with the following amended paragraph:

According to the above arrangement, in the encrypting ~~encryptin~~ device, keys g1 and g2 generated as a public key respectively include the power of (p-1) and the power of (q-1), and the ciphertext elements C1 and C2 generated using the public key {g1, g2} and the private key n also include the power of (p-1) and the power of (q-1), respectively. This makes it possible for the decrypting device to easily decrypt the ciphertext elements C1 and C2 using the Fermat's little theorem ($a^{p-1} \equiv 1 \pmod{p}$).